REMOVAL OF DATA FROM DECOMMISSIONED STORAGE DEVICES

Status:	**Active Policy**
Effective Date:	April 5, 2007 through April 4, 2009
Revised Date:	June 25, 2007
Approved By:	J. Stephen Fletcher, CIO
Authority:	*UCA §63F-1-206; Governor's Executive Order: Directing the Chief Information Officer to Develop and Implement Policy Promoting Security of State Information and Information Systems*

1.1 PURPOSE

To establish a policy and procedure detailing the criteria by which qualified Department of Technology Services (DTS) employees in authorized positions clear, erase, and remove all data and software from personal computers, file servers, and disk subsystems prior to decommissioning.

1.1.1 Background

External audits have identified the existence of data on hard drives in equipment designated to be surplused. This policy is intended to address the security risks associated with the unauthorized recovery of data from decommissioned equipment.

1.1.2 Scope

This policy and procedure applies to all personal computers, file servers, or electronic storage equipment supported, maintained, or administered by the DTS and the employees with responsibilities related to these devices. This policy also addresses the disposition of outdated or surplus information technology equipment, and the removal of all data and software from resident storage media devices.

1.1.3 Exceptions

Agencies excluded under the provisions of *§63F-1-102 (7) et seq.,* are not included under the provisions of this policy.

1.2 DEFINITIONS

Decommission
The process of removing sensitive and/or confidential programs or data files on computer storage media devices (e.g., hard drives, file server, disk subsystem, Blackberry device, USB drive) in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory efforts.

Information Assets
Information that is prepared, owned, received, or retained by a governmental entity that in its original form is reproducible by mechanical or electronic means.

Overwriting
The process of erasing, or "wiping," the contents of an electronic file or disk space. Overwriting of data means replacing previously stored data on a storage media device with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. It is virtually impossible to restore data on storage media that has been properly "wiped."

Physical Destruction
The physical destruction of storage media device is a process whereby the physical storage media is rendered useless and inaccessible. The end result is that individual "platters" of the storage media are completely destroyed or each platter has a minimum of three holes drilled through them.

Proof of Destruction
A certified statement and/or a detailed log completed and signed by the person who supervised the destruction of the storage media device.

Transfer
For the purposes of this policy, transfer means the physical removal or change of ownership of information technology equipment from an agency or the Executive Branch to another entity.

1.3 POLICY

1.3.1 All storage media that are supported, maintained, owned, or administered by DTS shall have all residing State of Utah data and software removed prior to the equipment's transfer or removal from State ownership.

1.3.1.1 Any evidence of ownership or use of the equipment must also be removed to ensure that no data of any type is left on the equipment.

1.3.2 All decommissioned equipment addressed in this policy must follow a uniform and consistent method for the removal of data and software from the storage media. The process will be performed for all departments and divisions whose information technology equipment is serviced by DTS.

1.4 DECOMMISSIONING AND DATA DESTRUCTION

There are two acceptable methods to be used for data destruction—Overwriting and Physical Destruction.

1.4.1 Overwriting

Overwriting is the primary and preferred method for data destruction. Overwriting software used by DTS personnel for data wiping must be endorsed by the State

Chief Information Security Officer (CISO). The CISO shall also maintain records of all personnel that are certified and trained to decommission storage devices.

1.4.2 Physical Destruction

Physical destruction is an alternative method for data destruction. With the approval of the Utah State Agency for Surplus Property (USASP) within the Division of Fleet Operations (see DAS Rule R28-1-4) DTS offices may physically destroy a storage media device.

1.4.2.1 In accordance with the DTS/USASP agreement, a storage media device that will not boot is preapproved to be physically destroyed. An SP-1 form shall be submitted to the USASP for the storage media device that is to be physically destroyed.

1.4.2.2 Processes used for the destruction and disposition of a storage media device must be endorsed by the department's Chief Operations Officer (COO) and CISO.

1.4.2.2.1 Information Asset Owners who want to physically destroy a storage media device, and the storage media device is not eligible for destruction under 1.4.2.1, shall be directed to complete and submit a Business Justification Form to the USASP. A storage media device shall not be destroyed without first obtaining approval from the USASP.

1.4.2.2.2 DTS offices that physically destroy a storage media device must follow a COO/CISO endorsed process.

1.4.2.2.3 DTS offices that physically destroy a storage media device must retain a proof of destruction. At a minimum, the proof of destruction must provide the serial number of the storage media device, the date of media destruction, the method(s) used to destroy the media (e.g., drilling, pulverizing, shredding), the vendor's name if a vendor was used to destroy the storage media, and the name, title and signature of the person who supervised the destruction of the storage media device.

1.4.2.2.4 When requested by the Enterprise Information Security Office (EISO) the proof of destruction for a storage media device must be provided to the EISO within 5 business days.

1.4.3 The EISO must provide training to assigned DTS staff and provide tracking documentation for use in the disposition and destruction of storage media devices.

1.5 PROCEDURES

All decommissioned equipment addressed in this policy must follow a uniform and consistent method for the removal of data and software from the storage media

device. The process will be performed for all agencies whose information technology equipment is decommissioned by DTS.

1.4.3.1 Identify equipment to be removed from inventory and prepared for decommissioning. This will be performed in conjunction with the agency being serviced by DTS.

1.4.3.2 Trained DTS staff will use CISO approved standard methods to decommission data storage media. Once decommissioning has been completed, no data (including an operating system) will reside on or be retrievable from the device.

1.4.3.3 Decommissioned equipment will be labeled with a DTS Data Removal Tag indicating that data has been cleared from the storage media. All decommissioned equipment will be documented on a Computer Equipment Media Disposal Form which tracks the type of equipment, serial number, tag number, if physical destruction was used to decommission the equipment a proof of destruction, name of the individual that performed the decommissioning, signature and date.

1.4.3.4 In conjunction with requirements of the USASP, an SP1 Form will be completed, by an assigned administrator, which will include the DTS Removal Tag numbers and serial numbers of all assets

1.4.3.5 An audit process, as defined and initiated by the CISO, will verify that the disposition of the decommissioned equipment is performed accurately.

1.4.3.6 If the storage media is inaccessible through electronic means, the media may be destroyed and rendered useless per the guidelines referenced in 1.4.2

1.5 APPENDICES

- Department of Defense (DoD) 5220.22-M guidelines
- Memorandum of Understanding between DTS and DAS for Surplus Property
- Utah Administrative Code R28-1-4

DOCUMENT HISTORY

Originator:	Dave Fletcher
Next Review:	May 10, 2009
Reviewed Date:	N/A
Reviewed By:	N/A